AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jack A. Vickery, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed for over twelve years. Prior to being employed by the FBI, I was a sworn law enforcement officer in the State of Georgia for approximately seven years. As an FBI Special Agent, I am currently assigned to the FBI Cleveland Division, Akron Resident Agency.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the activities of the person who utilized Kik username bk6755 with a display name Brad Kirkwood. As will be shown below, there is probable cause to believe that the user of Kik username bk6755 has received, possessed, and distributed child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I submit this application and affidavit in support of a search warrant authorizing a search of the residence located at 1575 8th Street, Cuyahoga Falls, Ohio, located in the Northern District of Ohio (the "Subject Residence"); a silver 2005 GMC Envoy bearing Ohio license plate GEU7414 registered to MATTHEW PASSALAQUA; a gold 1999 Mercury Grand Marquis bearing Ohio license plate GHL9586 registered to MATTHEW PASSALAQUA (collectively the "Subject Automobiles"); and the person of MATTHEW PASSALAQUA with a birth year of 1968 and a social security number ending in 2104 as further described in Attachment A. Located within the premises, the automobiles, and on the person to be searched, I seek to seize evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing transportation,

shipment, receipt, possession, distribution, and reproduction of child pornography. I request authority to search the entire premises, including the residential dwelling and curtilage thereof. I request authority to search any computer, computer media, and cellular telephone located in the premises, vehicle, and on the person to be searched where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of a crime.

4. The statements in this affidavit are based in part on information provided by the FBI's Springfield, Illinois field office and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of §§ 2252 and 2252A, are presently located at 1575 8th Street, Cuyahoga Falls, Ohio.

STATUTORY AUTHORITY

1. This investigation concerns alleged violations of Title 18, United States Code, §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors.

   a. Title 18, United States Code, Section 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of a minor engaging in sexually explicit conduct when such visual depiction was either mailed or, using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign

commerce.

b. Title 18, United States Code, Section 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or, using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

2. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic,

magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e- mail, remote storage, and co-location of computers and other communications equipment.

f. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers and/or letters separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. A creation IP address is the address used on the date that an e-mail or other account is created by the user.

g. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and

is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

h. A "wireless telephone" (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

i. "Mobile computing devices," are handheld electronic devices used for storing data (such as names, addresses, music, photographs, appointments or notes) and utilizing computer programs. Some mobile computers also function as wireless communication devices and are used to access the Internet and send and receive e-mail. Mobile computers often include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or

miniature hard drives. This removable storage media can store any digital data. Many users of these devices also use cloud storage applications to store data such as images and videos in order to back up data, duplicate data in order to access data from other devices, or to free up space on their device. Most mobile computers run computer software, giving them many of the same capabilities as personal computers. For example, mobile computers users can work with word-processing documents, spreadsheets, presentations, and internet browsing and chat applications. Mobile computers may also include global positioning system ("GPS") technology for determining the location of the device. Mobile computing devices include, but are not limited to, laptops, tablets and smartphones. This type of Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a mobile computer. As the amount of data that people store on their mobile devices has increased, smartphones and other mobile computing devices are also commonly synched with, or connected to, a desktop or laptop computer for backup data storage. This allows users to access selected data, such as photos, emails, contacts and documents, across multiple devices, or to recover this data if their mobile device is broken or lost.

j. A "digital camera" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various

types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

k. A "portable media player" (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

COMPUTERS AND CHILD PORNOGRAPHY

3. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. More recently, through the use of computers and the Internet, distributors of child pornography can use membership-based/subscription-based websites to conduct business, allowing them to remain relatively anonymous.

4. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child

pornography in these ways:

a. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as Charter Spectrum (formerly Time Warner), which allow subscribers to connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

b. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography

over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient.

c. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously within the last several years. These drives can store thousands of movie and/or image files at very high resolution.

BACKGROUND OF THE INVESTIGATION

5. This investigation was predicated upon an investigative referral from the FBI's field office in Springfield, Illinois based upon an undercover investigation on Kik Messenger. Kik Messenger, commonly called Kik, is a proprietary instant messenger software application (app) for mobile devices. It uses a smartphone's data plan or Wi-Fi to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content. Kik may also be accessed via laptop and desktop computers by downloading emulator software applications to these devices, such as Bluestacks or Andyroid. Kik is known for its features that preserve users' anonymity, such as allowing users to register without providing a telephone number, and preventing users from being located on the service (including by the company itself) through any information other than their chosen username. The app offers registered users the ability to initiate group chat, create Kik chat rooms, or to search for and join established KIK groups according to their interests.

6. On or about September 8, 2019, an FBI agent acting in an undercover capacity (hereafter "UC1") utilized Kik username "prvdad1980z" to post "Hey, perv dad here. anyone else

into taboo no limits, PM me", in a group chat titled "Boysfun Men Only" with group ID "Pe.doph", on the mobile messaging application Kik. UC1 received a private message from Kik user bk6755 with display name Brad Kirkwood.

7. Kik user bk6755 stated he was into no limits and family fun and mostly enjoyed talking about pictures. Kik user bk6755 expressed a sexual interest in UC1's purported ten year old son and eight year old daughter. Kik user bk6755 was interested in meeting, but lived near Akron, Ohio. Kik user bk6755 then wanted to talk about scenarios and asked UC1 if UC1 had a picture to talk about.

8. Kik user bk6755 then sent an image depicting a female child approximately eight to ten years old laying on her back with her legs spread open exposing her genitalia. Kik user bk6755 and UC1 conversed about how they both enjoyed the picture. Kik user bk6755 then sent another picture depicting a pubescent female approximately 15 to 20 years old fully nude laying on her back with an erect penis inserted into her anus.

9. During the course of several days, Kik user bk6755 sent UC1 multiple images and videos depicting child pornography or child erotic material. One such video depicted a child less than ten years old with hair shorter than shoulder length, wearing no shirt, pants, and socks. In the video, the child is seen using both hands to rub an adult male's erect penis.

10. On September 9, 2019, at 7:03:26 PM (UTC+0), Kik user bk6755 sent a video that depicted two male children approximately eight to ten years old, one of whom was in a complete stage of undress and in a seated position. The second child used one hand to rub the first child's erect penis. During the video, a female toddler entered the room and watched as the second male child opened and dropped his pants, exposing an erect penis. The naked male child then proceeded to use one hand to rub the other male child's penis.

While sending this video to UC1, Kik user bk6755 commented, "Look at this dude." Kik user bk6755 further described the video as "F***ing hot". UC1 asked where Kik user bk6755 found the video, to which Kik user bk6755 responded "Someone sent it".

11. On September 10, 2019, at 1:04:27 AM (UTC+0), Kik user bk6755 sent a video that depicted a male in a seated position, wearing a white t-shirt, and boxer shorts pulled down to expose his genitals. No other details of the male are visible. The male is seen masturbating until he ejaculates. Kik user bk6755 then indicated to UC1 that the male seen in the video was thirteen years old and that "this was live". The following date, UC1 asked Kik user bk6755 how he got "that live video from last night." Kik user bk6755 responded "Omegle. . . that's where I found that kid".

12. Based on investigations conducted by other FBI agents, as well as other investigators in the law enforcement community, I know that Omegle is a free online chat/ video conferencing Web site that randomly pairs users in one-on-one chat sessions where they can chat with strangers anonymously. I also know that Omegle is sometimes used to access and share child pornography. Based on the information available, it is not possible to determine if Kik user bk6755 recorded the video when it was live, or if he received the video from a third party.

13. On September 12, 2019, at 2:18:46 PM (UTC + 0), Kik user bk6755 then sent a live picture depicting a male approximately 40 to 50 years old, wearing glasses with a balding hair line. The picture was from the middle of the male's glasses to the top of the head. Kik user bk6755 also stated he worked at a grocery store.

14. On September 17, 2019, Kik Interactive responded to an administrative subpoena and provided subscriber data for user name bk6755[1].

    a. First Name: Brad

    b. Last Name: Kirkwood

    c. Email: hbsg3453@yahoo.com

    d. IP Analysis (ARIN whois): 70.61.42.126 and 173.89.92.218; Charter Communications

15. On September 20, 2019, Charter Communications responded to an administrative subpoena and provided subscriber data for the following IP addresses:

    a. 70.61.42.126 assigned on September 5, 2019 at 2:21PM UTC. The subscriber was Heinens with a subscriber address of 20 Shopping Plaza, Chagrin Falls, OH 44022.

    b. 173.89.92.218 assigned on September 5, 2019 at 11:40PM UTC. The subscriber was Heather Passalaqua with a subscriber address of 1575 8th Street, Cuyahoga Falls, OH 44221, email address hpassalaqua4@gmail.com, and telephone number 216-375-7602.

16. Open source checks revealed a MATTHEW PASSALAQUA, with a birth year of 1968, home address 1575 8th Street, Cuyahoga Falls, OH 44221. The checks also revealed a grocery store at address 20 Shopping Plaza, Chagrin Falls, OH 44022.

17. Social media checks revealed a Facebook page with user name Matthew Passalaqua. The pictures on the Facebook page were consistent with the image Kik user bk6755 sent to UC1.

[1] Kik Messenger does not verify the name provided by the Kik user.

18. On or about October 21, 2019, I confirmed through Ohio Bureau of Motor Vehicle (BMV) records that MATTHEW and HEATHER PASSALAQUA resided at 1575 8th Street, Cuyahoga Falls, OH 44221.

19. On October 21, 2019, I also queried the Cuyahoga Falls Police Department in Cuyahoga Falls, Ohio for any records of contact for the PASSALAQUAS. I was advised that there were no reports on file for MATTHEW PASSALAQUA, but Heather Passalaqua was listed as having contacted the Cuyahoga Police Department in 2017 and January of 2019. In both instances, Heather Passalaqua provided a contact phone number of 216-375-7602, which matched the records obtained from Charter Communications on 09/20/2019.

20. On October 21, 2019, at approximately 5:00 PM, I drove by 1575 8th Street, Cuyahoga Falls, OH 44221 and observed a GMC Envoy SUV parked in the driveway. The vehicle bore Ohio license plate GEU7414. I later confirmed through Ohio BMV records that this vehicle is actively registered to MATTHEW PASSALAQUA at 1575 8th Street, Cuyahoga Falls, OH 44221. Additionally, MATTHEW PASSALAQUA has 1999 Mercury Grand Marquis bearing Ohio license plate GHL9586 actively registered to him at that address.

21. Affiant knows that cellular telephones and mobile computing devices are popular due to their portability and can easily be transported and/or stored in an automobile.

DIGITAL TECHNOLOGY'S RELATIONSHIP TO CRIMINAL INVESTIGATION

22. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics

common to individuals involved in the receipt and attempt to receive child exploitation material and child pornography:

a. Those who receive and attempt to receive child pornography likely receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those that receive and attempt to receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal

such correspondence as they do their sexually explicit material; and often maintain contact information for individuals who share the same interests in child pornography.

e. Those that receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

23. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that MATTHEW PASSALAQUA, who resides at 1575 8th Street, Cuyahoga Falls, Ohio, as described in Exhibit A of this affidavit, is involved in possession and distribution of child pornography. I respectfully submit that there is probable cause to believe that PASSALAQUA has violated 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§, 2252 and 2252A, is located in the Subject Residence, the Subject Automobiles, and/or on the person of MATTHEW PASSALAQUA, and this evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

FORENSIC EVIDENCE

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can

sometimes be recovered with forensics tools.

25. As a result, I hereby request the Court's permission to seize the mobile computing devices and computers (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of such hardware for the evidence fruits and instrumentalities of violations of the Specified Federal Offenses.

26. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the Device and the application of knowledge about how the Device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. Often times users of a mobile computing device back up their device on a computer or use cloud storage applications to store data such as images and videos in order to back up data, duplicate data in order to access data from other devices, or to free up space on their device. Some examples of cloud storage applications are: Dropbox, OneDrive, and iCloud. Examination of the device may show evidence of cloud storage applications and accounts.

27. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of seized computers and devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

28. Based on the above information, there is probable cause to believe that the Specified Federal Offenses have been violated. Accordingly, I respectfully request that this Court issue a search warrant for the residence located at 1575 8th Street, Cuyahoga Falls, Ohio, located in the Northern District of Ohio (the "Subject Residence"); the silver 2005 GMC Envoy bearing Ohio license plate GEU7414 and the gold 1999 Mercury Grand Marquis bearing Ohio license plate GHL9586 (the "Subject Automobiles"); and the person of Matthew Passalaqua with a birth year of 1968 and a social security number ending in 2104, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, which constitute evidence, contraband, fruits, and other items related to violations of the Specified Federal Offenses.

Jack A. Vickery
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me this 12th day of November 2019.

Kathleen B. Burke
United States Magistrate Judge